コンバージしたアクセス（5760/3650/3850）の設定 外部Web 認証

目次

概要

この資料にコンバージしたアクセスコントローラで外部Web auth を設定する方法を定義されています。 ゲスト門脈ページおよび資格情報 認証はこの例の Identity Services Engine （ISE）に両方です。

前提条件

要件

次の項目に関する知識があることが推奨されます。

1. Cisco はアクセスコントローラ コンバージしました。

2. Web 認証

3. Cisco ISE

使用するコンポーネント

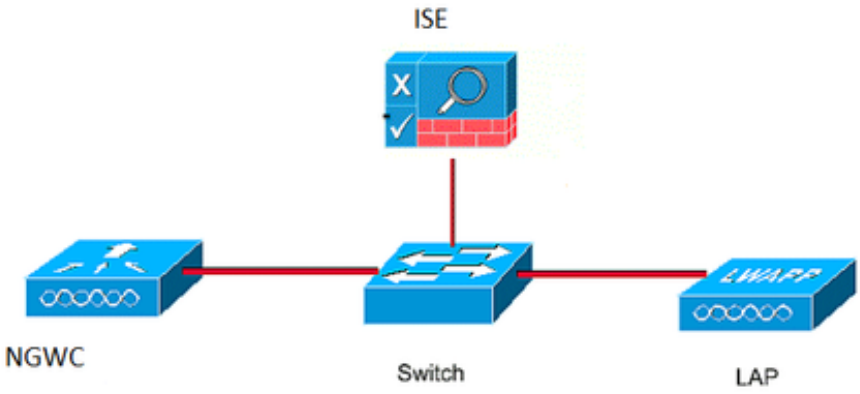
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

1. Cisco 5760 コントローラ（下記のダイアグラムの NGWC）、03.06.05E

2. ISE 2.2

設定

ネットワーク図



CLI 設定

コントローラの RADIUSコンフィギュレーション

ステップ 1： 外部 の RADIUSサーバを定義して下さい

```
radius server ISE.161
address ipv4 10.48.39.161 auth-port 1812 acct-port 1813
timeout 10
retransmit 5
key Cisco123
```

ステップ 2:。 AAA RADIUS グループを定義し、使用されるべき RADIUSサーバを規定 して下さい

```
aaa group server radius ISE-Group
server name ISE.161
deadtime 10
```

ステップ 3.半径グループを指すメソッドリストを定義し、WLAN の下でマッピング して下さい。

```
aaa authentication login webauth group ISE-Group
```

パラメータ マップ設定

ステップ 4.仮想 IP アドレスでグローバル な パラメータ マップを設定して下さい外部および内部 webauth に必要となる。 Logout ボタンはバーチャルIP を使用します。 その常にルーティングが不可能なバーチャルIP を設定する好ましい習慣。

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 1.1.1.1
```

ステップ 5： 指定されたパラメータ マップを設定して下さい。それは webauth 方式の型のように機能します。 これは WLAN 構成の下で呼出されます。

```
parameter-map type webauth web
type webauth
redirect for-login https://10.48.39.161:8443/portal/PortalSetup.action?portal=0c712cd0-6d90-
11e5-978e-005056bf2f0a
redirect portal ipv4 10.48.39.161
```

前に認証 ACL。 これはまた WLAN の下で呼出されます。

ステップ 6: 認証が終わる前に割り当てが ISE、DHCP および DNS にアクセスする Preauth_ACL を設定して下さい

```
ip access-list extended Preauth_ACL
permit ip any host 10.48.39.161
permit ip host 10.48.39.161 any
permit udp any eq bootps any
permit udp any any eq bootpc
permit udp any eq bootpc any
permit udp any eq domain any
permit udp any any eq domain
```

WLAN 構成

ステップ 7: WLAN を設定して下さい

```
wlan ext-webauth 7 ext-webauth
client vlan vlan232
ip access-group web Preauth_ACL
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauth
security web-auth parameter-map web
session-timeout 1800
no shutdown
```

ステップ 8: HTTPサーバをつけて下さい。

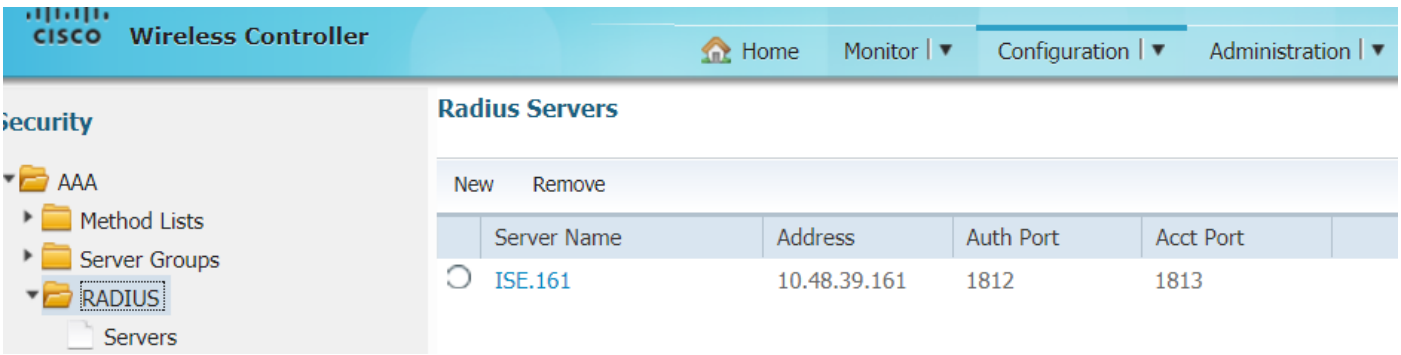
```
ip http server

ip http secure-server (for secure web-auth, use 'no' to disable secure web)
```

GUI 設定

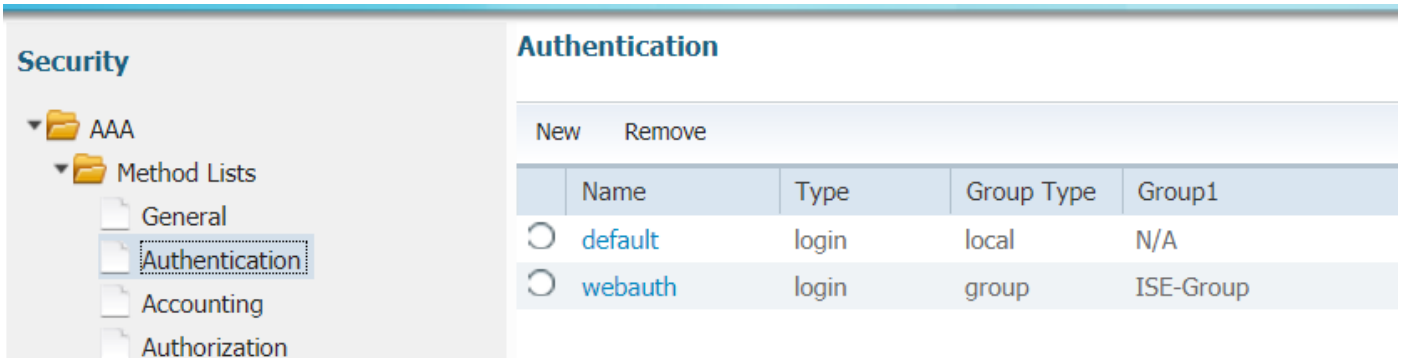
上でとここに次同じステップいます。 スクリーン ショットはクロスリファレンスにちょうど提供されます。

ステップ 1： 外部 の RADIUSサーバを定義して下さい



ステップ 2:。 AAA RADIUS グループを定義し、使用されるべき RADIUSサーバを規定 して下さい

ステップ 3.半径グループを指すメソッドリストを定義し、WLAN の下でマッピング して下さい。



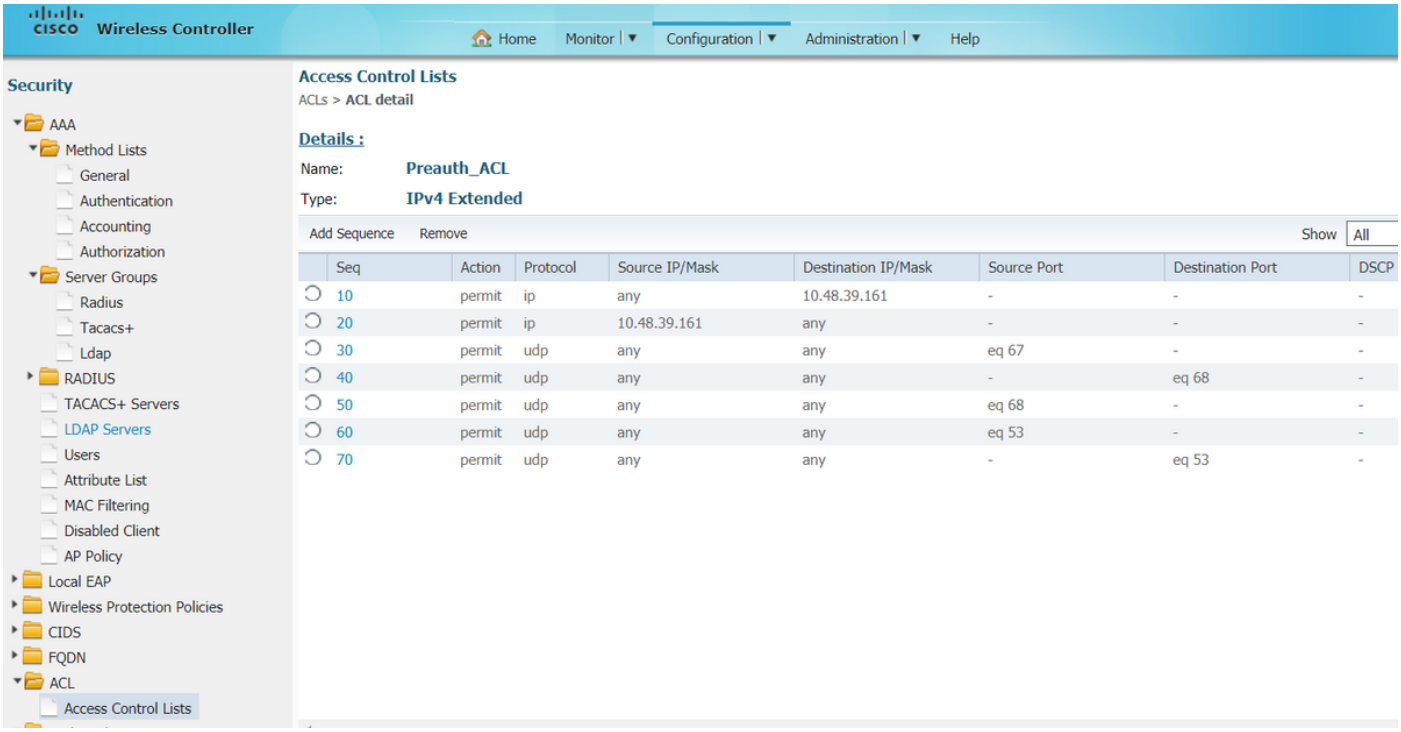
パラメータ マップ設定

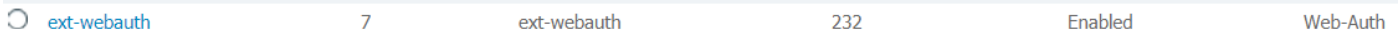
ステップ 4.仮想 IP アドレスでグローバル な パラメータ マップを設定して下さい外部および内部 webauth に必要となる。 Logout ボタンはバーチャルIP を使用します。 その常にルーティングが不可能なバーチャルIP を設定する好ましい習慣。

ステップ 5： 指定されたパラメータ マップを設定して下さい。それは webauth 方式の型のように機能します。 これは WLAN 構成の下で呼出されます。

前に認証 ACL。 これはまた WLAN の下で呼出されます。

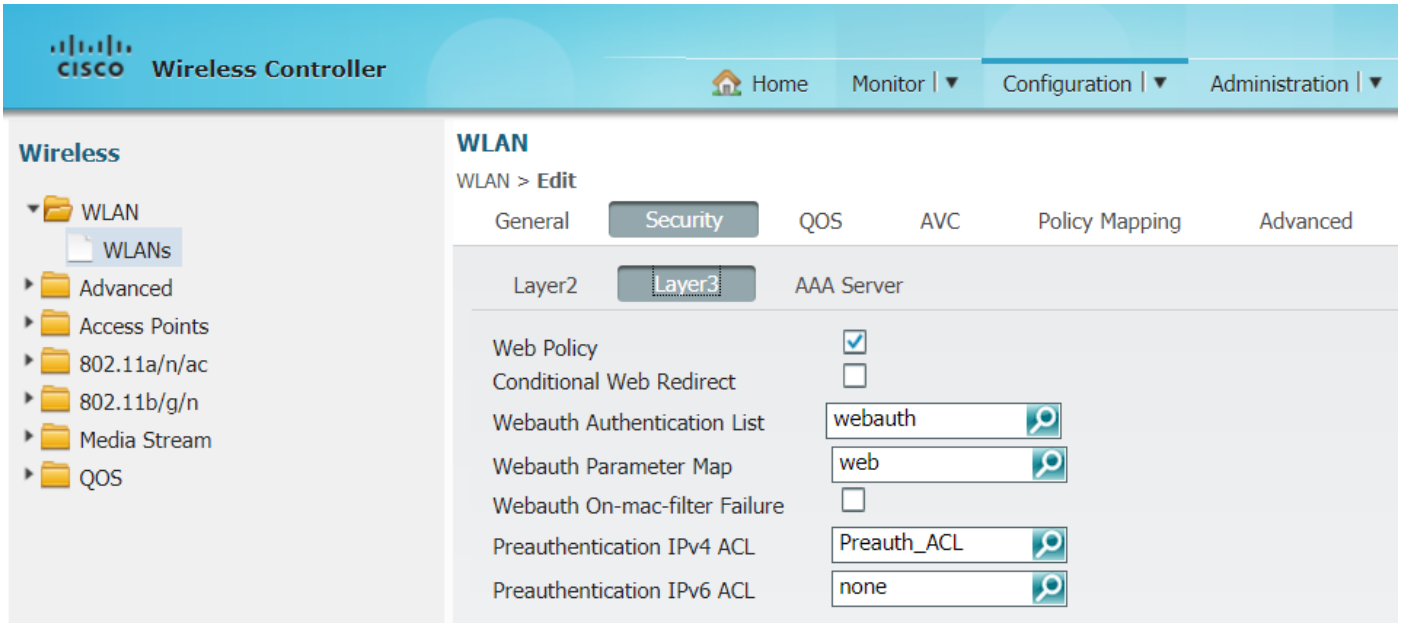
ステップ 6: 認証が終わる前に割り当てが ISE、DHCP および DNS にアクセスする Preauth_ACL を設定して下さい





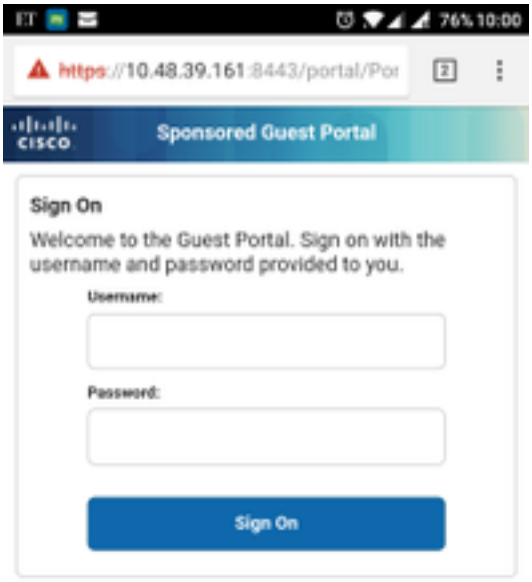
WLAN 構成

ステップ 7: WLAN を設定して下さい

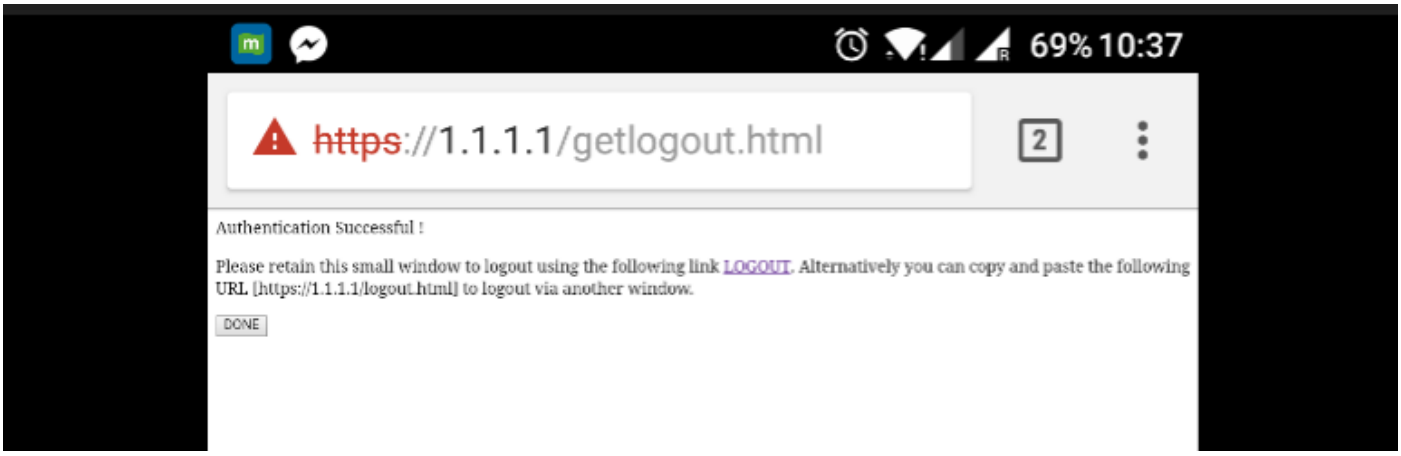


確認

ブラウザを開いたらクライアントを接続し、クライアントはログオン ポータル ページにリダイレクトされることを確かめて下さい。 下記のスクリーン ショットは ISE ゲスト ポータル ページを説明します。



適切な資格情報が入れば、成功ページは示されます:



ISE サーバは 2 に認証を報告します: WLC が RADIUS認証（このによって同じ ユーザ名/パスワードを認証だけ提供すれば guest ページの 1 つは自体（ユーザ名だけの要点）および第 2 認証 クライアントを成功フェーズに移動させます）。 RADIUS認証が（NAS として MAC アドレスおよび WLC 詳細と）行われない場合、RADIUSコンフィギュレーションは確認されるべきです。